

Game Theory on Fraud Syndrome of Internet Banking

Danny WC Ha, VP Certification (Hon.) of ICRM, FCRP, CRT, CISA, CISM, CISSP, CPM, CFE
Dr. Freddie PW Lee

[居安思危，思則有備，有備無患]: 作為卓越的管理人員，應該要警覺到將來可能發生的威脅或危機，作好準備去預防和面對。風險管理透過既定的程序，評估每個決策所帶來的影响，針討性地執行相應的行動和措施。[博奕論]是一個幫助企業實現策略目標的思考過程，一種基於資料的決策方法，面對抉擇的時刻，以邏輯性，數學性的方式，理性地考慮對手的選擇，定出有利的決策，致力於減低風險，改善產品及服務，降低風險成本，使顧客滿意及提高市場競爭力。本文將揉合博奕論的基礎，解析及討論網上銀行的欺詐行為，及資訊風險，讓管理人員了解風險管理的行動和措施，達至多贏最佳決策。


Introduction

In 21st century globalization and boundless context, there are known or unknown risks or crises that could cause immeasurable damage to an organization or the public. Executives must understand and develop the right win-win strategies to mitigate possible risks, and also the crisis response strategies for business recovery. This paper is designed to give a general insight into the application of Game Theory to manage and control the fraud syndrome with respect to the threats to internet banking and financial fraud.

What is game theory?

Game theory studies how people should act and interact in strategic settings. Game theory is optimal decision-making in the presence of others with different targets.

There are four parts to any game:

<ul style="list-style-type: none">• <i>A set of players</i>	
<ul style="list-style-type: none">• <i>Moves the players can make</i>	
<ul style="list-style-type: none">• <i>Results the players might achieve</i>	
<ul style="list-style-type: none">• <i>Nature of information about competitive activity</i>	

The players choose their moves to maximize their results. Each player always assumes that other players are also trying to maximize their score. Players often base their moves on what they think other people might do. Mathematics dominates much of formal game theory. In this paper, we propose the application of game theory to fraud syndrome in a way to keep the math to a minimum. Circumstances in business often arise where you would gain from making a “believable threat or promise”.

Game theory might sound esoteric, but we could see it as a way to analyze almost any kind of human interaction in which all the players, and other decision-makers, other entities or opponents want optimize their decisions. It is a very useful tool for looking at problems in that it could remove some of the fog on our minds. For details of game theory, please refer to the original documents.

“In a Nash Equilibrium, all of the players’ expectations are fulfilled and their chosen strategies are optimal.” – From a 1994 press release announcing the Nobel Prize winners in economics.

Fraud Facts

The three basic elements of fraud are:

- **Attitude:** A predisposition to commit fraud or an ability to rationalize fraudulent behavior.
- **Pressure:** Internal and external forces working on the individual that might influence their decision to commit fraud.
- **Opportunity:** Conditions that allow the fraud to take place.

In considering both the game theory and fraud elements above, the game players have to take the following factors into consideration for every strategic move.

- **Value:** What is the relative and maximum cost or value of the consequences of fraud?
- **Business Impact:** How do the consequences of fraud affect the ongoing operation of the business? What is the minimum and maximum magnitude of impact?
- **Control Environment:** How to provide discipline and structure proactively and/or reactively in an organization?



What are we waiting for?

To minimize the fraud syndrome, executives should consider the following questions:

- Does your organization currently do any of the “creative and proactive” approaches to carry out fraud prevention and detection?
- Would any of these approaches be difficult for you or your organization? What would be the possible obstacles and challenges?

- What is your organization's greatest fraud prevention opportunity? What action could be taken? How can you measure the overall performance of fraud prevention management?
- What do you believe should be the employees, risk management practitioner/audit department's role and responsibility in fraud prevention?

Internet Banking and Fraud

Banks, like any other companies or organizations, are taking risks in their daily operations. Managing risk plays a critical role in many areas of business and has huge implications in the banking industry in particular the internet banking business. The open nature of the Internet, Intranets and Extranets and sharing of data makes security a serious challenge. Until cost-beneficial solutions are found and properly implemented, banks and financial institutions engaging in internet e-commerce may continue to experience pains until there is some sure security strategies. Most importantly, it is to ensure that customers feel secure and have confidence and integrity on the internet banking.

The perpetrators (opponent) may be internal to a firm or an external hacker. The risks faced include theft of information, destruction, interception, alteration, stalling or rerouting of data, as well as forged messages. Stolen data may be used to defraud credit card companies of money or to learn trade secrets of competitors. The information necessary to penetrate a security system is often obtained from targeted collusive employees or what I call the "intelligence people" and/or social engineering. Best practice guidelines have to be developed to deal with such threats such as *Whistle blowing policies; Monitoring solutions; Policy and procedures review; Access rights and system controls; Procedures for dealing with offenders; and Interactive Training Program covering all elements from the guidelines.*

Phishing and transaction fraud are major high risk threats among many others including spyware, identity spoofing, cyber child labour, virus writing tools (script kiddies), and web-based systems vulnerabilities. Spamming is one of the media for Phishing and fraudulent scams. Cyber criminals, some of them are professionals, semi-professional, organized criminal groups (like Botnet) or criminologists, are launching attacks using calculated outcomes and carefully engineering technologies. They are more interested in making money and taking the risky approaches to set banks and financial institutions as their high-return targets. Security weaknesses of the banks internal communication networks is no longer the priority interest of attackers since it may need more time to overcome tightened security controls. They will choose the easy way. Value-added banking data of data-warehouse and business transactions are the major exposures to cyber criminals. This approach is reflected by 2005's syndrome of Phishing (identity theft) and financial fraud.

Crisis and risk management has to be an integral part of the overall strategy of any business in managing financial or credit risk, operational risk, outsourcing risk, audit risk, and legal risks on top of the information security risk in order to avoid regulatory penalties and survive in a highly competitive environment that filled with threats and uncertainties. Game Theory might be an exit.

Game Theory on Fraud Syndrome: Spamming

What is the Nash Equilibrium or “Spam Equilibrium” of spamming? We cannot have spam equilibrium if some spammer regrets not sending spam. If the cost of sending one million spam were one dollar, then a rational player would regret not spamming if it would earn the spammer more than one dollar. Importantly, everyone must not check inbox spam according to game theory rule. If even one percent of the public regularly read their spam, then it would clearly be worth for some spammers to spend one dollar to reach one percent of a million email users. More people will get spammed if one percent of us read spam. The best approach would be doing some technical controls that effectively separates out wanted email from spam like the anti-spamming services provided by some ISPs in Hong Kong.

Spamming would decrease if the cost to spammers be raised. If we impose legal penalties on spammers in Hong Kong, we will attract other countries spammers beyond the reach of local law. It is unlikely to get other countries to stop international spamming. International cooperation is sure a strategic move with mutual legal arrangements on extradition of offenders. Of course the United Nations system could be a “believable promise” for combating cyber crime and spamming. In 21st century globalization, boundless and collaboration context, moving to new equilibrium, we should consider if the new outcome would be a Spamming Equilibrium, otherwise, the new outcome is unreliable and might be difficult to achieve.

“Rather than ignoring what your opponent (now the criminal) is going to do or making a single assumption of what they’re going to do, you’re going to consider all possible reactions and then reason what the most likely action will be.”

“No player regrets his strategy, given everyone else’s move” – Nash Equilibrium

Privacy Syndrome

In the recent privacy disclosure crisis, game theory could also be helped to explain and provide possible exit. Many relevant elements could be plugged to the four parts of this the game of privacy syndrome.

- ***A set of players*** – law enforcement agency, outsourcing service provider, BT groups, citizens
- ***Moves the players can make*** – containment, report to public media, negligence, privacy law enforcement, spreading of privacy information, compensation
- ***Results the players might achieve*** – sensitive information disclosure, blackmail, imprison, extradition, scandal
- ***Nature of information about competitive activity*** – Any “creative and proactive” approaches to carry out fraud prevention? What would be the possible obstacles and challenges? What is your organization’s greatest fraud prevention opportunity? What action could be taken? How can you measure the overall performance of fraud prevention management? What do you believe should be the employees, risk management practitioner/audit department’s role and responsibility in fraud prevention?

It is your choice to select any or both of the following:

“No player regrets his strategy, given everyone else’s move” – Nash Equilibrium, Nobel Prize Winner in economics, 1994

"I already gave my best, and I have no regrets at all." – William Hang, American Idol, 2004 (William Hang might be a good player of game theory after 10 years.)

Regarding of how to handle the outsourcing risk and audit risk, one of possible solution could be the application of Game Theory and Six-Sigma to risk and crisis management plan. If the readers are interested to know more, please contact us.

Thank you. Mar 2006.

ICRM <http://www.icrmasia.com>

Contact: Mr. Danny Ha, iamokthankyou@gmail.com

*A paper for the 7th Info-Security Conference www.infosecurityproject.com
“Seamless Security Management for Today’s Banking and Financial Services”
Info-Security Handbook 2006
Organizer e21 Magicmedia
Hong Kong*